NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

Co-Chair: Dylan Gilbert, NIST Privacy Policy Advisor

MONTHLY MEETING MINUTES
Wednesday, September 13, 2023
1:00 P.M. ET – 2:00 P.M. ET

I. INTRODUCTION

The 27th meeting of the National Institute of Standards and Technology (NIST) Privacy Workforce Public Working Group (PWWG) convened on Wednesday, September 13th from 1:00 P.M. - 2:00 P.M. ET virtually via Microsoft Teams. There were 38 attendees.

The PWWG provides a forum for participants from the public, including private industry, the public sector, academia, and civil society, to create the content of the NIST Privacy Workforce Taxonomy. The PWWG is tasked with creating Task, Knowledge, and Skill (TKS) Statements aligned with the NIST Privacy Framework and the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.

PWWG Co-Chair, Dylan Gilbert, welcomed attendees and Project Teams Co-Leads and thanked them for their participation.

II. PWWG UPDATE

A. TIMELINE

The target timeline introduced earlier this year was to have the current project teams running from May through August and then launching the final 3 project teams in September. The final teams would then run from September to the end of the year with the goal of completing the work by the end of the calendar year. The NIST team was clear from the start that the timeline was aspirational. Efforts have been made to improve the process to speed things along as efficiently and quickly as possible. It is a group process and a long process by nature. The most important thing for the NIST team is to have a quality work product in the end. The work has fallen behind the initial target but not drastically. The current teams are making great progress, but they are not done. The target timeline has been slightly augmented.

The NIST team hopes to wrap up the current project teams by the end of October. It may be a time squeeze particularly for Project Team 8 because they have 10 Subcategories. Dylan is confident the adjusted target completion date for the current teams will be hit by at least one or more of the Project Teams. Afterward, the NIST Team will spin up the next three teams to work from the end of this year until early next year. The hope is to wrap up the last three teams around March 2024. The next three teams will have a staggered start. Whichever project team finishes first, likely Project Team 6 because they only have 3 Subcategories, will then be followed by the start of the next Project Team. The next Project Team to start will likely be Data Processing Awareness (CM.AW-P). Data Processing and Awareness (CM.AW-P) has eight Subcategories and will require more time than the others.

When the project teams are finished, a public draft of the taxonomy will be released. The core components of this taxonomy are going to be, at minimum, a list of the Task, Knowledge and Skill Statements that have been approved by the group. Additionally, there will likely be a mapping document which maps those Statements to the Subcategories in the NIST Privacy Framework Core. There will also be some front matter: a narrative to describe what this taxonomy is, how it got there, and how it can be useful. There will be a Knowledge and Skills Baseline, at minimum, which may be discussed in the front matter or in an appendix or possibly both. The Baseline will contain Knowledge and Skill Statements that are more broadly applicable to the entire Privacy Framework. The Baseline will be drafted once the project teams have completed their work and then put it out for public comment. Once the comments are in and adjudicated then NIST can release version 1.0 of the taxonomy, targeting next summer. The timeline will be augmented as necessary to get a quality work product out. Hats off to everyone for the great progress.

B. TKS COMPILATION DOCUMENTS – VERSION 5

The compilation documents are living documents that grow as the Task, Knowledge and Skill Statements are completed. Currently, within the compilation documents, there are Task, Knowledge, and Skill Statements from the first five Project Teams. As Project Teams Six, Seven and Eight finish their work those TKS Statements will be added to the compilation documents until it composes the entire taxonomy. Why is there a version five? Version five is indicative of the fact that it is a living document. It is growing and constantly revising. This past revision was a very big revision.

Currently there are over six-hundred Task, Knowledge, and Skills Statements that have been completed. The number will change and get bigger as more Task, Knowledge, and Skill Statements are done. There is a good chance there will be over one thousand TKS Statements when this is all said and done. It will be a very robust resource for the Privacy Community. The links to the compilation inventory and compilation mapping are available in the slide deck. The inventory and mapping documents are in the PWWG shared drive as well. It's a good resource especially if you are in a current Project Team and want to see the Tasks, Knowledge, and Skill Statements that have already been approved. There is no need to reinvent the wheel. The documents will provide a sense of what the Statements look like in their final form. Dylan will provide a live preview of the documents momentarily. Dylan acknowledged the great work done by Wendy Szwerc from the PWWG team. Wendy led on the most recent update which was a lot of work.

C. TKS STANDARDIZATION

What does it mean to standardize the TKS Statements? There will still be slight variations in the way that a Statement is written despite the NIST Authoring Guidance. The NIST team wants to avoid that and standardize the Statements as much as possible, so they are grammatically and syntactically correct. The standardization involves basic line edits for syntax and authoring guide conformity. The PWWG Team is leveraging the NICE style guide from our colleagues on the NICE Framework Team for further standardization. The NICE Framework Team are doing the same process with their Task, Knowledge, and Skill Statements. To the extent that there are differences or rules specific to the PWWG then those will be put in place and carried forward.

D. EXAMPLES OF TKS STANDARDIZATION

What are some of the examples of things that we have done?

1. How can we avoid multiple TKS Statements for common phrases in the PF (e.g., policies, processes, and procedures)?

Some of the teams have been grappling with certain phrases that show up a lot in the Privacy Framework, often with commas, such as, 'policies, processes, and procedures' and 'mission, objectives, and activities.' To adhere to the Authoring Guide, multiple Statements are required for these, one Task for policies, one for processes, etc. The solution employed is to utilize slashes with these commonly occurring phrases which would enable them to be grouped together.

Examples of these combined Statements:

- Knowledge of how system/product/service inventories are organized.
- Knowledge of existing policies/processes/procedures.

2. How should TKS Statements generally refer to stakeholders?

Dylan noted that anyone who has participated in a project team will recognize that the term, "stakeholders", comes up frequently. They often need to be collaborated with or consulted or identified when it comes to achieving outcomes in the Privacy Framework. There were many varied ways of referencing Stakeholders in the TKS Statements. The Team decided upon a standardized format, organization-defined parameters, which will be familiar to those who use Special Publication (SP) 800-53 (Rev 5). SP 800-53 is a consolidation of privacy and cybersecurity controls which has been mapped to the Privacy Framework. The PWWG taxonomy will use the bracketed term, [*organization-defined stakeholders*], to note that it's up to the organization to define the stakeholders in each context. This provides maximum flexibility for organizations.

The following PWWG Task Statement conforms to this rule:

- Finalize privacy policies with approval from [*organization-defined stakeholders*].

Dylan noted that there will always be exceptions, and one exception in the Privacy Framework is where it specifically calls out third-party stakeholders, such as:

- Identify third-party stakeholder roles and responsibilities to support privacy policies/processes/procedures.

In this case, it's necessary to specify that there are third-party stakeholder roles without specifying who the third-party stakeholders are.

The rule is not completely set in stone. If the group thinks this should be avoided in the future for whatever reason, a different approach can be implemented. For now, the team thinks this is the best way to efficiently handle this problem.

3. How can we streamline statements that contain assumed knowledge or activities?

As the team reviewed the totality of the Statements which contained knowledge or activities which they think should be assumed, they wanted to pull those things out of the Statements and define and address the assumed knowledge and activities within the taxonomy and put it either in the front matter or in an appendix. As an example, a Statement relating to establishing organizational roles where necessary and feasible to support third parties, stakeholder privacy, and risk management responsibilities. Generally, most of this can be pulled out and it will say, unless otherwise indicated, assume that this is referring to the organization. Also assume that a Task is necessary to do that.

An example of this would be:

- **Example Old "Assumed Knowledge" Statement:** Establish organizational roles, where necessary and feasible, to support third-party stakeholder privacy risk management responsibilities.
    - **Example Updated "Assumed Knowledge" Statement:** Establish a role(s) to support third-party stakeholder privacy risk management responsibilities.

There are going to be places where we will need to call out certain things, so we're being careful to make sure that we don't eliminate Statements where this information is applicable, as in the following example:

- **Example: Retained "Organization Specific" Statement:** Knowledge of the organization's contract management practices (e.g., storage, location, responsible entity).

In addition to assumed knowledge would be assumed activities. There's will be certain things to assume within our statements that we can call out again up front, or make sure that it's known when organization 'X' is using the PWWG Workforce Taxonomy. In the next example of an assumed activity, 'document organizational privacy values', and 'maintain documentation of organizational privacy values', there was a lot of conversation around this early on. It was decided to view this as an assumed activity.

- **Example Old "Assumed Activity" Statements:**

  Document organizational privacy values.
  Maintain documentation of organizational privacy values.

    - **Example Updated "Assumed Activity" Statement:** Document organizational privacy values.

E. TKS STANDARDIZATION – KNOWLEDGE AND SKILLS BASELINE

Knowledge and Skill Statements have been removed from the compilation documents because the NIST Team and Co-Chairs think they are better suited for what is being called a Knowledge and Skills Baseline. They will be Knowledge and Skills that are so broadly applicable to everything within the Privacy Framework that it's not useful to just map it everywhere. It is more useful to provide a set of things that one needs to know and the skills one needs to have if you are going to use the Privacy Framework. They will probably be located in front matter and/or in an appendix. Dylan thinks it is worthy of a conversation with the group of what this should look like in terms of how much of it should be narrative, and how much of it should be graphical content. The NIST Team wants to ensure that things are easily digestible and made accessible for anyone utilizing it. To be further discussed toward the end of the timeline when the work of the Project Teams end.

- **Examples of broadly applicable Knowledge and Skills:**
    - Knowledge of privacy laws, regulations, standards, and best practices and skill in applying them.
    - Collaboration and Communication Skills

Dylan took a moment to pause for questions from the members.

Question: A member inquired if Dylan thinks a final and comprehensive baseline would be completed around January/February of 2024?

Dylan noted it is being built in real time. The NIST Team does not want to close the door on making changes to it prematurely. He anticipates it will be finalized closer toward the end of the line when the Project Teams are wrapping up before drafting up the initial public draft. He is optimistic that there will not be a lot of change at that time. Hopefully, the group will be able to identify gaps at that time and ask what is missing and what clearly belongs in the baseline that is not in it. The intention of the NIST Team is to come out of the gate with a comprehensive baseline.

F. TKS STANDARDIZATION – LIVE WALK THROUGH OF TKS STATEMENT COMPILATION DOCUMENTS, VERSION 5

Dylan provided a live walk through of the TKS Compilation Inventory and the TKS Compilation Mapping.

The first document Dylan shared was the TKS Compilation Inventory document. The Statement type is listed in the far-left column which are color coded based on their type (Task, Knowledge, or Skill). The middle column lists the ID number. Finally, the Statement itself is in the right column. The Statements are alphabetized within each Statement category which is the most intuitive way to organize these Statements when listing them out. The alphabetizing resets at the start of a new type of Statement.

Changes of note are the slashed terms like, policies/processes/procedures. Parentheticals are employed within the Statements. Parentheticals provide additional guidance for a user of the taxonomy to think about what they may need to do. Also included are the organization-defined parameters. Instead of having ten Statements that work as variations on a theme, it made more sense to use a robust organization defined parameter. The parameter provides flexibility to the organization. Dylan requested the members review the document and provide comments prior to the release for public comment.

Dylan shared the TKS Compilation Mapping document. The mapping document takes past Knowledge and Skills Statements from the Inventory and maps them to a given Subcategory in the NIST Privacy Framework based on how the project teams assigned them. The mapping can be helpful for bundling in the Task, Knowledge, and Skill Statements within the taxonomy to an organization’s privacy framework implementation.

G. TKS STANDARDIZATION – NEXT STEPS

Dylan noted that there is still one Subcategory within the Risk Assessment Category for which the Task, Knowledge and Skill Statements are being finalized. It is the AI flavored Subcategory. They have been working with their NIST colleagues for some time to get that set of TKS Statements completed and are just finishing it up. NIST hopes it will be done by the October call and ready for discussion.

The NIST team will also be standardizing the material from Project Teams 6, 7 and 8. Dylan has been taking steps to implement these types of things in with the current batch of statements. They will work on a style guide, in addition to the Authoring Guide. It will include considerations for people to employ while putting together material.

They will also take some additional looks at the compilation documents to see if there are other places to consolidate additional statements.

III. Project Team Updates

A. UPDATE OF PROJECT TEAM 6: RISK MANAGEMENT STRATEGY

GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

- **Risk Management Strategy (GV.RM-P)**: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
  - **GV.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.
  - **GV.RM-P2**: Organizational risk tolerance is determined and clearly expressed.
  - **GV.RM-P3**: The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.

Team Lead James Koons provided the update for PT6. Project Team 6 has completed GV.RM-P1. It was an interesting learning curve with a lot of great discussion. Meeting attendance has had a lot of fluctuation which probably contributes to the slower progress. Currently focused on GV.RM-P2. Except for the Skill Statements, the team is soon to complete this Subcategory. There were a couple of Task and Knowledge Statements that were still outstanding, but James has formatted them for the group. Hopefully on the next call the team will finish up the remaining Skill Statements in P2 and move onto P3. James has learned a lot and continues to learn a lot about how this works. The momentum should pick-up.

Team Lead Dana Garbo agreed with James. There is an art to the progress, but the NIST team has been extremely helpful. As a Co-Lead Dana finds a challenge being that it is very easy to do the obvious and keep repeating oneself. The Knowledge and Skills Baselines will be very important in making it all come together nicely.

James noted the importance of this being a collaborative effort. If there are any team members on the call James would like to remind them that they may add comments within the document. The system promotes collaboration for multiple people to work on it simultaneously. The comments that have been provided have been very thought provoking and helpful.

B. UPDATE OF PROJECT TEAM 7: Awareness and training (GV.AT-P)

GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

- **Awareness and Training (GV.AT-P):** The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.

  - **GV.AT-P1**: The workforce is informed and trained on its roles and responsibilities.
  - **GV.AT-P2**: Senior executives understand their roles and responsibilities.
  - **GV.AT-P3**: Privacy personnel understand their roles and responsibilities.
  - **GV.AT-P4**: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.

Project Team 7 Co-Lead, Jacqueline Crowley provided the team update for PT7. The team has completed work on TKS Statements for GV.AT-P1. The goal for this work period is to continue pre-drafting the TKS Statements for GV.AT-P2 through P4. The Co-Leads are working on ensuring that they don't have redundant Statements. It has taken longer than anticipated but they have had great support from the NIST Team.

Elif noted that they created many Tasks for P1 with which they are very happy. Early on it was highlighted that some terminology was not clear for the team members. The Team Leads were tasked to come up with standardized definitions for some key terms. Those operational definitions are:

- **Awareness and Training Program** – The overall initiative that includes but is not limited to learning outcomes, the awareness and training plan, and resources (i.e., people, technology, funding).
- **Awareness and Training Plan** – A document that outlines the strategic approach and specific details (e.g., activities, materials, communications plan, delivery mechanisms) of the awareness and training program.
- **Awareness and Training Activity** – A component of the program carried out to execute the plan (e.g., "Intro to Privacy" course, tabletop exercise).
- **Awareness and Training Material** – A learning resource associated with the program (e.g., incident reporting poster, job guide, newsletter).

When initially creating these Statements, it was necessary to come to a common understanding.

Dylan noted that there has been a lot of challenges and discussion around P2-P4 due to the unusually worded Subcategories within the Privacy Framework. Instead of being a passive, 'workforce is informed and trained', for example, there is an active voice outcome such as 'executives understand their roles and responsibilities', etc. It was a challenge for members to create Tasks that get to this understanding and furthermore, given that we are doing a bunch of things with P-1, due to role-based training, are we not just going to be completely duplicative?

There was a lot of interesting discussion about this. They landed on two things. First, it is important to think about the work around the Privacy Framework considering other Frameworks. These outcomes are either taken directly from or slightly adapted from the NIST Cybersecurity Framework which is undergoing a big update to Version 2.0. Given that we will have different outcomes for a while, plus the idea of potentially duplicative Tasks between P1, P2-P4, the team concluded that there will not be many Tasks required for P2-P4. Focus can be applied toward looking at what are the Knowledge and Skills particular for this specialized training necessary to call out. Dylan noted it took about a month of debate to work through toward that conclusion. All this work and debate is important because now the team is confident about where it stands, and the rest can be efficiently and quickly created.

C. UPDATE OF PROJECT TEAM 8: DATA PROCESSING MANAGEMENT (CT.DM-P)

CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

- **Data Processing Management (CT.DM-P**): Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).

  - **CT.DM-P1**: Data elements can be accessed for review.

- **CT.DM-P2**: Data elements can be accessed for transmission or disclosure.
- **CT.DM-P3**: Data elements can be accessed for alteration.
- **CT.DM-P4**: Data elements can be accessed for deletion.
- **CT.DM-P5**: Data are destroyed according to policy.
- **CT.DM-P6**: Data are transmitted using standardized formats.
- **CT.DM-P7**: Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.
- **CT.DM-P8**: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.
- **CT.DM-P9:** Technical measures implemented to manage data processing are tested and assessed.
- **CT.DM-P10**: Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.

Project Team 8 Co-Lead, Abby Palia, provided the update. The team has completed TKS Statements for CT.DM-P1. Meeting attendance has been consistent. The Team Leads appreciate the contributions and work of all who have contributed thus far.

Next steps for PT8 are to work on P2-P4. Subcategories P1-P4 are nearly identical so the PT8 Team Leads plan to work on P2-P4 internally offline. The Leads will take a first pass at filling in P5 later this afternoon and begin working on P5 with the whole team tomorrow during their scheduled meeting.

In terms of the remaining subcategories, P6-P10, which cover topics like transmitting, auditing, processing, and disruption, there remains a lot of work to do. Abby requested members review the Subcategories and leave comments in the workbook.

Dylan noted that one of the benefits of this Subcategory, as Abby mentioned, is that there are a lot of variations on a theme within the first four Subcategories. Dylan believes those can be considered completed. The PT8 team is now at the hallway point. If anyone has a passion for data destruction now is the time to join PT8. Dylan's impression of this work is that people have many different opinions of how this gets done at any given organization which is a challenge. The goal is saying that given everyone has a slightly different job to do how does the team level that up into a place that is flexible and broadly applicable while also being useful. Dylan thinks the team is doing an exceptional job of landing on where they need to be. He looks forward to seeing how they work through the second half of the Subcategories.

IV. Q & A

V. NEXT STEPS & UPCOMING MEETINGS

A. NEXT STEPS

Join a project team! The mailing lists are now live. Sign up for any team or all of teams! The team Leads will soon send out a welcome note via the Google Group mailing list.

- PT6 (GV.RM-P): PrivacyWorkforcePT6+subscribe@list.nist.gov
- PT7 (GV.AT-P): PrivacyWorkforcePT7+subscribe@list.nist.gov
- PT8 (CT.DM-P): PrivacyWorkforcePT8+subscribe@list.nist.gov

B. UPCOMING MEETINGS

The upcoming meetings of the NIST PWWG and its Project Teams are noted below. For further information, including updated meeting schedules, meeting minutes, agendas, and slide deck please visit the PWWG web page.

Project Team 6 (PT6)

- Next Meeting: Thursday, September 21, 2023 | 1:00pm – 2:00pm ET

Project Team 7 (PT7)

- Third Meeting: Wednesday, September 20, 2023 | 1:00pm – 2:00pm ET

Project Team 8 (PT8)

- Third Meeting: Thursday, September 14, 2023 | 11:00am – 12:00pm ET

NIST Privacy Workforce Public Working Group

- Wednesday, October 11, 2023 | 1:00pm – 2:00pm ET

C. NEW BUSINESS OPEN TOPICS

New Business Open Discussion Topics Drop Box is available on the NIST Privacy Workforce Working Group webpage. If you are interested in presenting a business topic during a PWWG Monthly Meeting, please visit the webpage noted above.

D. TROUBLESHOOTING

If you have any technical issues with meeting invitations, mailing lists, and/or accessing the Google Drives, please email NIST PWWG Support at PWWG@nist.gov.

E. JOIN MAILING LIST

To join one of the Project Teams you must subscribe to its associated mailing list. All mailing lists are moderated. Please be reminded to adhere to the Mailing List Rules that can be found on the NIST Privacy Workforce Working Group website.

- PWWG: PrivacyWorkforceWG+subscribe@list.nist.gov
- PT6 (GV.RM-P): PrivacyWorkforcePT6+subscribe@list.nist.gov
- PT7 (GV.AT-P): PrivacyWorkforcePT7+subscribe@list.nist.gov
- PT8 (CT.DM-P): PrivacyWorkforcePT8+subscribe@list.nist.gov